Canadian Security Intelligence Service

Service canadien du renseignement de sécurité

SECRET

January 23, 2017

To: All employees

From: Deputy Directors Operations

Subject: **Project**

In early October, the Federal Court issued a judgement further to a series of hearings, known as the "*en banc* hearings". The majority of the judgement dealt with the Service's long term retention of associated data; however the Federal Court also responded positively to our request for a number of changes to section 21 (s. 21) warrant conditions.

(For more information on the judgement see the Director's November 3rd message (French) or the General Backgrounder here (FRENCH).

To implement the changes to the warrant conditions, we will be required to modify some of our s. 21 business practices and Project has been established to ensure that this is done in a coordinated fashion across the Service. Much of the work is well-underway and we anticipate changes to certain warrant conditions beginning in early-March. A Directive will be sent out with further details and, beginning in early-February, the DDO Secretariat and Project team members will hold information sessions with stakeholders across the country to explain any new compliance procedures.

Should you have questions, you may contact the team via their email address or call the Team's Lead, at extension

I would like to take this opportunity to thank you in advance for your support of this initiative.

Deputy Director Operations

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Director - Directeur

PROTECTED
April 12, 2017

TO: All employees

FROM: Director Coulombe

SUBJECT: **Action Plan: Addressing Practices in Warrant Matters raised by the Federal Court**

In early November, I wrote to your regarding a decision by the Federal Court of Canada on warrant conditions and the retention of non-threat related associated data linked with third party communications. That decision also found that CSIS breached its duty of candour in not informing the Court about its data analytic programme and its policy on the retention of associated data. In the same message, I also outlined that the Service had accepted the Court's decision and that we would be working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court going forward.

To that end, the Government of Canada (GC) retained the services of two accomplished legal experts. Murray Segal, a former Deputy Attorney General of Ontario, with an extensive background in criminal law, was retained to provide advice regarding best practices in warrant matters. Former Deputy Minister of Justice and Deputy Attorney General of Canada, John Sims, Q.C. was retained to provide advice regarding implementation of the Segal Report, and in effectively managing and conducting warrant applications before the Federal Court.

After receiving this extensive advice, CSIS and the Department of Justice (DoJ) undertook a number of measures aimed at improving their practices in applying for warrants under s. 21 of the *CSIS Act* in the Federal Court resulting in the development of a joint CSIS and DoJ policy. Some changes have already been implemented, some are in the process of being implemented, and others will be implemented in the near future. Highlights of the measures taken are summarized in the action plan, and organized according to six broad themes: accountability, governance, scanning, responsiveness, training and facilitating the work of the Court.

I invite you to please take the time necessary to familiarize yourselves with this material. Maintaining the confidence of the Government and the Canadian public requires that we demonstrate our commitment to complying with the requirements set out in law and in Ministerial Direction. Compliance enables us to support accountability and demonstrate our integrity, while preserving our operational authorities and effectiveness.

P.O. Box 9732, Station "T", Ottawa, Ontario K1G 4G4 | C.P. 9732, Succursale "T", Ottawa, Ontario K1G 4G4

Achieving a robust compliance culture within the Service depends on more than just processes, policies, and supporting technologies. It depends on people, and success will be driven by increased employee awareness, engagement and commitment.

Thank you,

Michel Coulombe
Director

Segal Report Summary
Sims Report Summary

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT
REVISE PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCES A L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT
REVISE PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCES A L'INFORMATION

Canadian Security Intelligence Service
Service canadien du renseignement de sécurité

Director - Directeur

UNCLASSIFIED
November 3, 2016

TO: All employees

FROM: Director Coulombe

SUBJECT: **Federal Court's Decision on Retention of Associated Data**

Recently, messages were shared on *The Source* pertaining to the restriction of access to certain datasets and data analysis capabilities. This action was prompted by a recent Federal Court of Canada decision on warrant conditions and the retention of non-threat related associated data linked with third party communications. When CSIS intercepts communications under a warrant, it obtains the content of the communication, as well as data about the communication. This can include things such as phone numbers, time, and location among others. Previously, CSIS practice had been to delete the content of communications intercepts collected under warrant assessed to be non-threat related, but retain all of the associated data. Data exploitation by the Operation Data Analysis Centre (ODAC) employs computers to analyze associated data and discover new linkages, trends and patterns critical to investigations.

In the ruling released today, the Federal Court recognized the intelligence value of the data analytic programme, and did not question the legality of collecting telecommunications associated data pursuant to warrants. However, on the very specific issue of retaining non-threat related associated data linked to third-party communications, the Court found that that associated data can only be retained if it is related to threats or of use to an investigation, prosecution, national defence or international affairs.

We accept the Court's decision in full and have taken immediate actions to respond. As previously communicated, CSIS has halted all access to, and analysis of, associated data. At this time, no associated data will be deleted, but it is unavailable for analysis. The Court's finding means that CSIS will be required to assess, within a short period, communications data to determine its relevance to a subject of investigation or threat to the security of Canada.

It is important to note that at no time did the Service believe the retention of non-threat related third party associated data to be inconsistent with the *CSIS Act*. Nor were we conducting these data analytic activities surreptitiously.

The decision also found that CSIS breached its duty of candour in not informing the Court about its data analytic programme and its policy on the retention of associated data. CSIS had informed Ministers, the Inspector General, the Privacy Commissioner and the Security Intelligence

Review Committee of our data analysis program, activities and the existence of ODAC. The Service accepts the Court's ruling on the issue of candour and we are working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court going forward.

Importantly, the Court acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology. The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy, and has the tools and authorities, with appropriate oversight, to meet both. CSIS will continue to contribute to that dialogue when possible to ensure we maintain the confidence of Canadians in our ability to balance these priorities.

As such, I invite you to read our public response to the Court's decision through our media statement and Backgrounder. The retention and analysis of information is a significant public policy issue, not just in Canada, but also among our closest allies, and it can be a complicated technical subject. To help further clarify the issue in question, the Service will also be providing a background briefing to journalists.

We will be undertaking a thorough review of the Federal Court's decision on the retention of non-threat related associated data linked to third parties in order to assess the potential operational and legal impacts. The Executive and I are committed to keeping all employees up-to-date on developments as we determine our way forward. Employees are encouraged to speak with their supervisors should they require any clarification or support.

Michel Coulombe

Qs & As

Qs & As

A. THE FEDERAL COURT DECISION

1. Why did the Director appear before the Federal Court?

- Late 2015, CSIS applied to renew and obtain new warrants as well as propose amendments to warrant conditions.

- In light of the finding in the Security Intelligence Review Committee's (SIRC) annual report (2014-15), the Court requested that the collection, use, retention and destruction of associated data (referred to by SIRC as metadata) collected under warrants also be addressed.

2. What is the decision?

- The Court agreed with most of the terms and conditions proposed by CSIS on the warrant application that was presented to the Court.

- The Court found that CSIS failed to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC), but did not find evidence that this had been done deliberately.

- The Court determined that CSIS' retention of associated data linked to third-party communications found to be unrelated to threats or of no use to an investigation, prosecution, national defence or international affairs, is illegal.

- That said, it is important to underline that all associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' long-term retention of non-threat related associated data linked with third party communications, after it was collected.

- Further, the Court rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.

3. This is not the first incident of CSIS being found to be in breach of Duty of Candour. Why and what is being done to address this?

- CSIS recognizes the importance of openness and transparency with the Federal Court.

- Over time, the provisions of the warrants have changed to take into account the evolution of technology, legal developments and investigative measures.

- The *CSIS Act* defines the Service's relationship with the Court. The means to approach the Court is through a warrant application, which creates a very focused type of interaction.

- We take these concerns very seriously and are working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.

- The Attorney General of Canada has taken a number of steps, including receiving advice from external experts, to ensure they are in the best possible position to meet the Government's duty of candour in future hearings.

4. Why did CSIS not inform the Court of its new position on the retention of data and the creation of the Operational Data Analysis Centre (ODAC)?

- At various points, the Government, the Security Intelligence Review Committee and the Office of the Privacy Commissioner were made aware of CSIS' position on the retention of data and the establishment of ODAC.

- In June 2011, CSIS did advise the Federal Court that it amended the wording of warrant conditions, but the Court found that our submission did not adequately address the distinction between the content of communications from the associated data of communications. CSIS accepts this finding.

- CSIS acknowledges the fact that the Court should have been informed earlier of the existence of ODAC, and the change in the retention policy, and acknowledges this was a significant omission. At no point did CSIS deliberately seek to withhold this information from the Court, and the Court acknowledged that there is no evidence to that fact.

- The development of this new capability evolved over time, as has our understanding of our obligations towards the Federal Court in this regard, which CSIS determines in close consultation with the Department of Justice.

5. Has CSIS briefed this Minister on this matter?

- In the context of an update on the court hearing, the current Minister of Public Safety has been briefed a number of times.

- At various points, previous Ministers, the Security Intelligence Review Committee and the Office of the Privacy Commissioner were made aware of CSIS' position on the retention of data and the establishment of ODAC.

6. Did CSIS purposely mislead the Court in this case?

- Government officials did not deliberately mislead the Court. The Court found that CSIS failed to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC), but did not find evidence that this had been done deliberately.

CSIS RESPONSE TO THE DECISION

7. What have you done to respond to the judgement?

- On duty of candour: We take this finding very seriously and recognize the importance of compliance with Ministerial Direction and the *CSIS Act*, as well as openness and transparency with the Court.

- We can and will do more to ensure that CSIS is fully transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court issued warrants. To that end, the Service is working closely with the Department of Justice.

- On the retention of non-threat related associated data linked with third-party communications: CSIS immediately halted access to, and analysis of, associated data until such time as it can successfully distinguish associated data linked to third-party communications from that of subject of investigation communications.

8. What steps will CSIS take to implement the Court's recommended two-step process of assessment?

- CSIS will be required to assess, within a short period, communications data to determine its relevance to a subject of investigation or threat to the security of Canada.

- Significant efforts will be required to implement policies, processes and technology that will successfully distinguish between threat related and non-threat related associated data.

9. Has CSIS destroyed the data deemed illegal by the Court?

- The Court did not order CSIS to destroy third-party associated data from its databases and recognized that the retention and analysis of associated data has yielded useful intelligence results in the past.

- CSIS immediately halted analysis and use of all associated data until such time as it can successfully distinguish associated data from that linked to a threat.

- We are assessing the application of the Court's finding in this regard.

CSIS USE OF ASSOCIATED DATA, ODAC

10. How will CSIS deal with the associated data it currently holds?

- CSIS immediately halted all access to, and analysis of, all associated data until such time as it can successfully distinguish associated data from that linked to a threat.

11. Do data exploitation technologies target individuals NOT engaged in threat related activity?

- No. Data exploitation is used in response to specific operational queries related to mandated investigations.

- Data exploitation is a tool to assist the Service in discovering linkages, trends and patterns to advance investigations.

- Determining whether or not a communication is threat-related is complex and may only become apparent as an investigation progresses.

- The Service has seen examples where communications originally assessed to have no intelligence value were later revealed to contain key threat-related information.

12. What is data exploitation, how does CSIS conduct data exploitation and why?

- Data exploitation employs computers to analyze data and discover linkages, trends and patterns. These techniques enable humans to make sense of volumes of information that could not be processed without a computer's assistance.

- Data exploitation enables the Service to effectively analyze threats to the security of Canada over time. It can provide insight into subjects of investigation; identify new leads and intelligence gaps and provide context and understanding to operations.

- The exploitation of data is invaluable in relation to the exercise of CSIS' mandate, but it must be undertaken responsibly and in accordance with our authorities. The Federal Court decision provides new direction in this regard.

13. Was SIRC aware of CSIS' data exploitation activities and collection of associated data?

- SIRC was aware of CSIS' data exploitation activities from shortly after the establishment of ODAC in 2006.

- The Inspector General was also provided a verbal briefing on ODAC and data exploitation in support of operations in 2011.

- SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal.

14. What were the Service's practices with regard to the retention of data collected under warrant prior to the Federal Court's decision?

- Pursuant to policy, one year after collection, CSIS practice was to delete the content of communications intercepts collected under warrant assessed to be of no intelligence value.
- Though the content was destroyed, the data about the communication was retained, whether or not it was related to a third-party.

FEDERAL COURT HEARINGS

15. What is an "en banc" hearing, why are they being held in relation to national security issues and what was the Government's role?

- These are hearings where all available designated judges of the Federal Court, may attend, participate, and hear evidence. The Federal Court of Canada determines when en banc hearings occur. Very rarely, the Court has requested that a warrant application be heard in the presence of most or all designated judges.

- As stated in Justice Noel's decision, sitting en banc in this case was helpful in reaching a decision as he had the benefit of his colleagues' perspectives.

- Counsel for the Attorney General attended these hearings to represent CSIS in relation to specific warrant applications.

Service News

ODAC – communications metadata analysis

October 14, 2016

To all Service employees,

For the time being, the website by which employees can access ODAC data will be taken offline. Furthermore, ODAC will not be able to perform any data exploitation on section 21 metadata in relation to intercepted communications of targets until further notice.

This action stems from the recent Federal Court en banc decision which characterizes Service's retention of non-target, non-threat-related metadata as illegal. The Service is currently reviewing this decision, and determining its way forward.

Please note that the Court's decision will not stop the Service's use of metadata analysis in support of investigations; however, we will have to revise our practices to ensure compliance with new conditions established by the Court.

DG

Access to S.21 related metadata

October 30, 2016

To: All Service employees

Further to the message on Section 21 related metadata, ITSS has restricted access to metadata in the following repositories and related systems until further notice;

DG ITSS

Nouvelles du Services

CADO - l'analyse des métadonnées de communication

Le 14 octobre 2016

À tous les employés du Service

À compter d'aujourd'hui, le site web du Centre d'analyse des données opérationnelles (CADO) sera mis hors ligne. De plus, le CADO ne sera plus en mesure d'exploiter des métadonnées tirées de l'interception de communications (article 21), et ce jusqu'à nouvel ordre.

Cette mesure découle de la récente décision de la Cour fédérale, en formation plénière, selon laquelle la conservation de métadonnées non attribuées à des cibles et qui ne sont pas liées à la menace est illégale. Le Service examine la décision, afin de déterminer la voie à suivre.

La décision de la Cour ne cessera pas l'analyse des métadonnées à l'appui des enquêtes du Service. Cependant, nous devons revoir nos pratiques, afin de respecter les nouvelles conditions établies par la Cour.

DG

Accès aux métadonnées reliés à l'article 21

Le 30 octobre 2016

A : tous les employés du Service

Suite au message de la concernant l'utilisation des métadonnées reliés à l'article 21, jusqu'à nouvel ordre, la DSSTI a supprimée les accès aux métadonnées dans les répertoires et systèmes suivants;

DG DSSTI

TRANSMITTAL SLIP / NOTE D'ENVOI

To / À	Classification
DIR	PROTECTED
From / De	File / Dossier
ADP	
Drafting officer / Rédacteur	Date
CB	2017 04 06

Subject / Sujet

SOURCE MESSAGE FROM DIRECTOR RE. SIMS AND SEGAL REPORTS ON DUTY OF CANDOUR

Action / Donnez suite	Priority / Priorité	Deadline / Délai
☐ Signature ☐ Comments / Commentaires ☑ Approval / approbation ☐ Information	☐ Routine ☐ Urgent ☐ Immediate / Immédiate	**MONDAY, APRIL 10, 2017**

Record of Consultation / Rapport de consultation	Concur D'accord Yes / Oui	Concur D'accord No / Non	Comments / Commentaires
DG CB Apr 16, 17	X		ADP, As requested, CB has prepared a message from the DIR for when the Segal and Sims summary reports, as well as the Action Plan and joint policy are posted publicly by the Department of Justice. Date currently TBC. DG CB

OK
2017.04.11

CB CCM# ~~17444~~ 17466

Protected
April 7, 2017

TO: All employees

FROM: Director Coulombe

SUBJECT: **Action Plan: Addressing Practices in Warrant Matters raised by the Federal Court**

In early November, I wrote to your regarding a decision by the Federal Court of Canada on warrant conditions and the retention of non-threat related associated data linked with third party communications. That decision also found that CSIS breached its duty of candour in not informing the Court about its data analytic programme and its policy on the retention of associated data. In the same message, I also outlined that the Service had accepted the Court's decision and that we would be working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court going forward.

To that end, the Government of Canada (GC) retained the services of two accomplished legal experts. Murray Segal, a former Deputy Attorney General of Ontario, with an extensive background in criminal law, was retained to provide advice regarding best practices in warrant matters. Former Deputy Minister of Justice and Deputy Attorney General of Canada, John Sims, Q.C. was retained to provide advice regarding implementation of the Segal Report, and in effectively managing and conducting warrant applications before the Federal Court.

After receiving this extensive advice, CSIS and the Department of Justice (DoJ) undertook a number of measures aimed at improving their practices in applying for warrants under s. 21 of the *CSIS Act* in the Federal Court resulting in the development of a joint CSIS and DoJ policy. Some changes have already been implemented, some are in the process of being implemented, and others will be implemented in the near future. Highlights of the measures taken are summarized in the action plan, and organized according to six broad themes: accountability, governance, scanning, responsiveness, training and facilitating the work of the Court.

I invite you to please take the time necessary to familiarize yourselves with this material. Maintaining the confidence of the Government and the Canadian public requires that we demonstrate our commitment to complying with the requirements set out in law and in Ministerial Direction. Compliance enables us to support accountability and demonstrate our integrity, while preserving our operational authorities and effectiveness.

Achieving a robust compliance culture within the Service depends on more than just processes, policies, and supporting technologies. It depends on people, and success will be driven by increased employee awareness, engagement and commitment.

Protégé
Le 7 avril 2017

À : Tous les employés

DE : Michel Coulombe, directeur

OBJET : **Plan d'action : pratiques concernant les questions liées aux mandats soulevées par la Cour fédérale**

Au début de novembre, je vous ai écrit au sujet d'une décision rendue par la Cour fédérale du Canada relativement aux conditions énoncées dans les mandats et à la conservation des données qui sont liées aux communications de tiers mais qui n'ont pas trait à la menace. La Cour fédérale a aussi déclaré que le SCRS a manqué à son obligation de franchise en omettant de la mettre au courant de son programme d'analyse des données et de sa politique sur la conservation des données liées aux communications. Toujours dans le message de novembre, j'ai précisé que le SCRS avait accepté la décision de la Cour et que, de concert avec le ministère de la Justice, il s'efforcerait de trouver des moyens de veiller dorénavant au respect de ses obligations envers la Cour.

À cette fin, le gouvernement du Canada s'est assuré les services de deux grands hommes de loi. M. Murray Segal, ancien sous-procureur général de l'Ontario qui a un impressionnant bagage dans le domaine du droit criminel, a été embauché pour fournir des conseils sur les pratiques exemplaires concernant les questions liées aux mandats. De plus, M. John Sims, c.r., qui a déjà été sous-ministre de la Justice et sous-procureur général du Canada, a quant à lui donné des conseils sur la mise en œuvre des recommandations du rapport Segal et sur la façon efficace de gérer et de présenter des demandes de mandats à la Cour fédérale.

Forts de tous ces conseils, le SCRS et le ministère de la Justice ont entrepris la mise en œuvre d'une série de mesures afin d'améliorer la façon dont ils présentent à la Cour fédérale des demandes de mandats au titre de l'article 21. Ces efforts ont mené à l'élaboration d'une politique commune au SCRS et au ministère de la Justice. La mise en place de certains changements est terminée alors que pour d'autres, elle a été amorcée ou le sera sous peu. Le plan d'action présente succinctement les principales mesures prises, qui sont divisées en six grands thèmes : reddition de comptes, gouvernance, balayage, capacité de réaction, formation et facilitation du travail de la Cour.

Je vous invite à prendre le temps nécessaire pour vous familiariser avec ce document. Pour conserver la confiance du gouvernement et des Canadiens, nous devons démontrer que nous sommes déterminés à respecter les exigences énoncées dans la loi et dans les instructions du ministre. La conformité nous permet d'appuyer la reddition de comptes et de démontrer notre intégrité en plus de conserver les pouvoirs qui nous sont accordés et de préserver notre efficacité opérationnelle.

La mise en place d'une culture plus solide en matière de conformité au sein du Service ne repose pas que sur les processus, les politiques et le soutien technologique. Elle repose également sur les personnes. La clé du succès : des employés plus sensibilisés, mobilisés et dévoués.

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

STATEMENT

CSIS Director statement regarding decision of the Federal Court

Ottawa, Thursday, November 3, 2016 - The Director of the Canadian Security Intelligence Service (CSIS), Michel Coulombe, issued the following statement regarding the decision issued today by the Honourable Justice Noël of the Federal Court:

"The Federal Court has recently ruled on the retention of associated data linked to third party information. CSIS fully accepts the Court's decision, and has taken immediate actions to respond. Given the Court's decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.

I regret that we did not meet our duty of candour to the Court, and I commit to continuing my efforts, with the Deputy Minister of Justice, to address the Court's concerns. Let me be clear: all associated data collected under warrant was done so legally. The Court's key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected.

CSIS, in consultation with the Department of Justice, had interpreted the *CSIS Act* to allow for the retention of this sub-set of associated data. It is now clear that the Federal Court disagrees with this interpretation; a decision which we fully accept.

As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to analyze associated data and enhance its capacity to identify and assess threats to the security of Canada over time. When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool. In the ruling released today, the Federal Court recognized the intelligence value of the data analytic programme and did not question the authority of collecting telecommunications associated data pursuant to warrants. The Court also rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.

The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy, and has the tools and authorities, with appropriate oversight, to meet both.

P.O. Box 9732, Postal Station "T", Ottawa, Ontario K1G 4G4
C.P. 9732, Succursale "T", Ottawa, Ontario K1G 4G4

Canada

Because the nature of our business is principally secret, Canadians are largely unaware of the professionalism and outstanding dedication the men and women of CSIS show every day as they carry out intelligence work. As the Director of CSIS, I am extremely proud of the people with whom I work. Canadians, too, should be proud of those who work tirelessly to keep this great country safe.

In addition, with respect to the ongoing situation in Quebec regarding the surveillance of journalists, I would like to state that I agree fully with the Prime Minister's statement on this matter. Such a situation would not occur at the federal level given the strong safeguards and protections we have in place to protect the freedom of the press in the course of our business.

We appreciate the confidence the government has in CSIS, and it remains for us a privilege to protect Canadians and Canada's interests at home and abroad."

-30-

Information:
Media Relations
Canadian Security Intelligence Service
media-medias@smtp.gc.ca
613-231-0100

P.O. Box 9732,
Postal Station "T"
Ottawa, Ontario
K1G 4G4

C.P. 9732,
Succursale "T"
Ottawa, Ontario
K1G 4G4

Canada

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

BACKGROUNDER

Federal Court ruling on the retention of associated data linked to third party information.

- CSIS takes seriously the concerns expressed by the Court with respect to meeting our duty of candour, and recognizes the importance of openness and transparency with the Federal Court.

- CSIS is working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.

- The Canadian Security Intelligence Service is mandated to investigate activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. In order to investigate these threats, CSIS may apply to the Federal Court for a warrant when the response to the threat requires more intrusive measures.

- Through the proceedings of the Court, over time, the provisions of warrants have changed to take into account the evolution of technology, legal developments, and investigative measures.

- This ensures that the powers granted by the warrants are clearly defined and that their conditions take into account the impact that the execution of the warrant has on the collection and the retention of information.

- The decision relates to the retention of certain information that has been legally collected via the execution of warrants, issued by the Court, which authorized the interception of communications.

- CSIS had sought to fully analyze all of the information - both the content and the associated data - for example, email addresses and telephone numbers.

- As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to significantly enhance the identification and assessment of threats to the security of Canada over time and space. This includes identifying patterns of movement, communications, behaviours, broad trends, and links that are otherwise unidentifiable.

P.O. Box 9732
Postal Station "T"
Ottawa, Ontario
K1G 4G4

C.P. 9732
Succursale "T"
Ottawa, Ontario
K1G 4G4

Canada

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

- When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool.
- In the ruling released today, the Federal Court recognized the intelligence value of the data analytic programme and did not question the authority of collecting telecommunications associated data pursuant to warrants.
- On the very specific issue of associated data linked to third-party communications, the Court found that it can only be retained if it is related to threats or of use to an investigation, prosecution, national defence or international affairs.
- CSIS, in consultation with the Department of Justice, had interpreted the *CSIS Act* as enabling the retention of this sub-set of associated data to allow for that important analytic work. At no time did the Service believe this to be inconsistent with the *CSIS Act*.
- It is now clear that the Federal Court, on the issue of the retention of certain data, interprets the *Act* differently.
- We accept this decision and have taken immediate actions to respond.
- In response to the decision, CSIS halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.

P.O. Box 9732
Postal Station "T"
Ottawa, Ontario
K1G 4G4

C.P. 9732
Succursale "T"
Ottawa, Ontario
K1G 4G4

Canada